UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with the Google Accounts fortunatefutures.org@gmail.com, fortunatefutures7@gmail.com, and fortunatefutures8@gmail.com that is stored at premises controlled by Google LLC

Case No. 23 MJ 133

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1035 and 1347	False Statements Related to Healthcare and Healthcare Fraud

The application is based on these facts:

See Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI SA Jill Dring
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 8/3/2023

Judge's signature

City and state: Milwaukee, Wisconsin

William E. Duffin
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jill Dring, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google, LLC, an electronic communications provider headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since March of 2013. As a Special Agent, I investigate civil and criminal matters related to health care fraud involving violations of the Health Care Fraud Statute, False Claims Act, Anti-Kick Back Statute and Stark Law. Prior to investigating health care fraud matters, I investigated criminal and national security related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of SPAM, malicious software, the theft of identification information, and other computer-based fraud. I have received training in computer technology and computer-based fraud and health care fraud.

3. The facts in this affidavit are known to me through my personal knowledge, training, experience, and through information provided to me by other law enforcement officers in the course of their official duties, whom I consider to be truthful and reliable.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. § 1320a-7b (Illegal Kickbacks) have been committed by Demaryl R. HOWARD (DOB: 03/25/1972), the owner of Fortunate Futures, and others known and unknown to the case agents. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated.

PROBABLE CAUSE

Background about Medicaid and the PNCC Program

7. By way of background, a Prenatal Care Coordination (PNCC) agency provides services that are reimbursed under Wisconsin Medicaid. The purpose of the PNCC benefit is to provide access to medical, social, educational, and other services to pregnant women who are considered at high risk for adverse pregnancy outcomes. The components of this benefit are

outreach, assessment, care plan development, ongoing care coordination and monitoring, and health education and nutrition counseling.

8. PNCC services are reimbursed under Wisconsin Medicaid when provided in accordance with Wisconsin Medicaid's rules and regulations. Covered services related to PNCC services are listed in Wis. Admin. Code § DHS 107.34.

9. When enrolling in Wisconsin Medicaid, the owners of PNCCs sign a provider agreement. By signing that agreement, the provider acknowledges that every time the provider submits a claim, he or she is certifying that he or she has not offered, paid, or received any type of illegal remuneration in violation of 42 U.S.C. § 1320a-7b, Wis. Stat. § 946.91(3).

10. The PNCC program requires providers to submit accurate and truthful claims for payments. It also requires a provider to only seek reimbursement for the actual amount of time spent assisting a member. And it prohibits providers from seeking reimbursement for noncovered services. Examples of non-covered services include personal comfort items such as radios and television sets. DHS 107.03(6). Additionally, DHS has explained that if a client is in need of something like diapers or wipes, a care coordinator should connect the client with an organization that can provide those items, rather than providing them. The PNCC program prohibits seeking reimbursement for noncovered services by charging for a covered service that was not actually provided.

11. Wisconsin Department of Health Services (DHS) maintains an online portal that allows for the submission of allegations of fraud involving Wisconsin Medicaid-funded providers. This online portal assists DHS in its mission to identify and investigate Wisconsin Medicaid fraud. DHS performs its own investigation. When deemed necessary, DHS forwards these investigations

as credible allegations of fraud to the Medicaid Fraud Control and Elder Abuse Unit (MFCEAU) to prosecute civil and criminal offenses related to the Wisconsin Medicaid program.

12. Per Wis. Admin. Code § DHS 107.34, PNCC agencies are required to work with a Qualified Professional. Prior to services being performed for a Medicaid recipient by a PNCC, and the subsequent reimbursement by Wisconsin Medicaid, the PNCC must complete an initial assessment and care plan with the client. The Qualified Professional either completes that assessment him or herself, or reviews and signs the assessment.

Demaryl Howard and Fortunate Futures

13. Demaryl Howard is the owner of Fortunate Futures, a PNCC located at 3020 W. Vliet Street in Milwaukee, Wisconsin. Fortunate Futures first enrolled as a PNCC agency on or about December 26, 2015.

14. In May 2022, the DHS Office of the Inspector General ("DHS OIG") performed an onsite record collection at the office of Fortunate Futures. Based on the inspectors' observations and records received (described below), the DHS OIG believed Fortunate Futures was billing for services that were not actually rendered.

15. First, although DHS requested records for 36 members, Fortunate Futures provided enrollment and care plans for only four. These members had care plans dated in 2018 and 2019 that all lacked the signature of a Qualified Professional. Fortunate Futures was unable to provide care plan records (or enrollment records) for the remaining 32 members.

16. Second, Fortunate Futures provided progress notes (which describe services purportedly provided to members) for 35 members. DHS OIG reviewed these notes and identified the following concerns:

a. Progress notes were written for a member, T.C-C., who was deceased at the time services were purportedly provided to her. The member passed away on August 21, 2021, but there were seven progress notes for 14 hours of services purportedly provided from August 21, 2021 to September 18, 2021.

b. Some progress notes were identical for multiple different members.

c. Some progress notes were identical for the same member for multiple months.

d. Some progress notes appeared copied with members' name and dates added.

e. The amount of time purportedly spent provided services appeared inflated.

17. Finally, many services listed on the progress notes appeared to be out of the scope of the benefit program and therefore would be non-covered services, not eligible for reimbursement from Medicaid.

18. On or around May 26, 2022, based on the findings described above, DHS OIG referred the matter to MFCEAU for investigation of a credible allegation of fraud.

19. As part of MFCEAU's investigation, MFCEAU Investigator Rory O'Sullivan obtained the death certificate of T.C-C., who passed away on August 21, 2021 from "hemorrhagic shock" due to, or as a consequence of, "uterine rupture."

20. Investigator O'Sullivan also confirmed through Fortunate Futures' billing records that Fortunate Futures billed Medicaid for services that were purportedly provided to T.C-C. on August 31, 2021 and September 18, 2021.

Use of Google Email Accounts

21. On September 23, 2022, Demaryl Howard was served with a subpoena requesting all records of Fortunate Futures, to include any and all correspondence relating to daily business operations, including but not limited to notes, emails, memos, letters and recordings. The response

from Howard included business-related emails sent to and from the following email addresses: FortunateFutures7@gmail.com, FortunateFutures8@gmail.com, and FortunateFutures.org@gmail.com (the "Target Accounts").

22. For example, on May 24, 2020, the email address fortunatefutures.org@gmail.com was used to send an email to Demaryl Howard and Pongella Welsh. The subject line stated, "Meeting this Thursday." The email began, "Dear Fortunate Futures Care Coordinators." The email was written by Tamara Thompson (aka Tamara Thompson Howard), Executive Assistant for Fortunate Futures.

23. On October 6, 2020, Ruben Hopkins, Coordinator for Fortunate Futures, used the email address fortunatefutures8@gmail.com to send an email to fortunatefutures7@gmail.com. The content of the email was several attachments titled, "Fortunate Futures Online and In-Person Training Update", "Fortunate Futures Online EVV Orientation Training Schedule" and "Fortunate Futures Staff Email List Full Version."

24. On June 25, 2021, Ruben Hopkins used the email address fortunatefutures8@gmail.com to send a message addressed to "Everyone" notifying them that their billing was past due if not completed already and that the office would be open the following day for individuals to drop off their billing. DemitaPrescott@yahoo.com responded to this email inquiring about payday.

25. On July 21, 2021, Ruben Hopkins, fortunatefutures8@gmail.com sent an email to Lanina Winters, copying fortunatefutures7@gmail.com. The content of the email requested verified demographic information for a client, which was needed before Medicaid could be billed for services. Similar emails were sent to other care coordinators.

26. On August 6, 2021, Ruben Hopkins, fortunatefutures8@gmail.com sent an email to Demaryl Howard, fortunatefutures7@gmail.com. The content of the email included a database with staff email addresses. The spreadsheet listed care coordinators and their clients.

27. On August 10, 2021, Ruben Hopkins, fortunatefutures8@gmail.com, sent an email addressed to "Everyone." In the email, Hopkins stated that on Saturday there would be a Back to School Backpack Give Away for "the clients we serve." Fortunate Futures had about 100 backpacks to give away on a first come, first served basis.

28. On July 21, 2021, Ruben Hopkins, fortunatefutures8@gmail.com sent an email addressed to "Hello Team!" The email was a reminder that all billing was due.

29. On August 16, 2021, Ruben Hopkins sent an email addressed to "Everyone," informing them of a staff meeting that would be held on August 20, 2021. The agenda for the meeting was client services – events, information, support, billing – timely submission, and staff training – care plan updates.

30. On October 11, 2021, Ruben Hopkins, fortunatefutures8@gmail.com, sent an email with several dates regarding care coordinator training. Demaryl Howard, fortunatefutures7@gmail.com responded with "Looks great Rube!! Let's do it!"

31. Based on these email messages, and the investigation to date, there is probable cause to believe that Howard and others associated with Fortunate Futures used the Target Accounts to communicate about billing, at least some of which I suspect to be fraudulent, based on what DHS OIG investigators and Investigator O'Sullivan discovered, described above, and kickbacks, such as gifts to potential clients.

BACKGROUND CONCERNING EMAIL

32. In my training and experience, I have learned that Google, LLC provides a variety of on-line services, including electronic mail ("email") access, to the public. Google, LLC allows subscribers to obtain email accounts at domain names of their creation, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC asks subscribers to provide basic personal information. Therefore, the computers of Google, LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, LLC subscribers) and information concerning subscribers and their use of Google, LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. A subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, LLC In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

34. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to

identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

35. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

36. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

38. Based on the forgoing, I request that the Court issue the proposed search warrant.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google, LLC Because the warrant will be served on Google, LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with fortunatefutures.org@gmail.com, fortunatefutures7@gmail.com, and fortunatefutures8@gmail.com ("the Target Accounts") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on 2/22/2023 with **the Google Reference Number 31168666,** Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **December 26, 2015** to **the present**, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and
8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

Google is hereby ordered to disclose the above information to the government within **14** (fourteen) days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. § 1320a-7b (Illegal Kickbacks), occurring on or after December 26, 2015, including, for example, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence demonstrating a scheme to defraud Wisconsin Medicaid;

b. Evidence demonstrating the provision of kickbacks in exchange for medical services and/or billing;

c. Evidence of communications regarding how to conduct billing or avoid detection of billing fraud;

d. Communications between or among HOWARD and other people participating in the fraud;

e. Communications with clients;

f. Evidence indicating how and when the Account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crimes under investigation and to the Account owner;

g. Evidence indicating the Account owner's state of mind as it relates to the crimes under investigation;

h. The identity of the person(s) who created or used the Account;

i. The identity of the person(s) who communicated with the Account about matters relating to health care fraud and illegal kickbacks.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in

addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.